

CONSTRUINDO UM FIREWALL NO LINUX CENTOS 5.7

Sumário

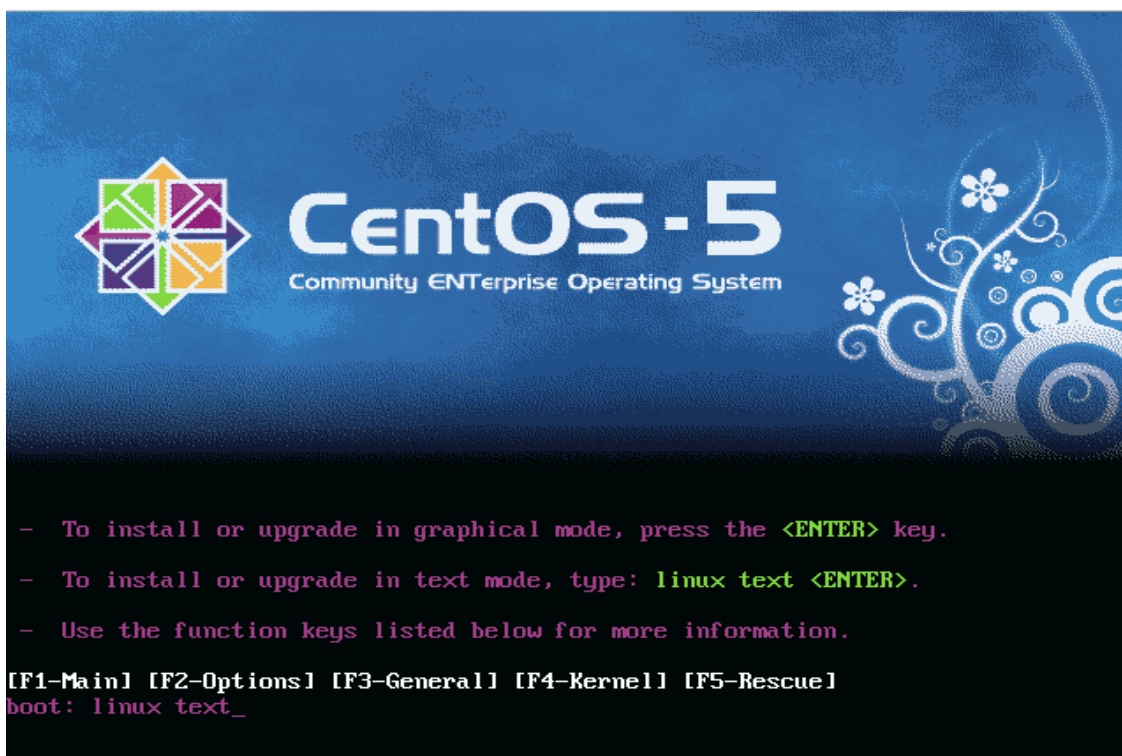
1 INSTALANDO CENTOS.....	3
2 INSTALANDO SERVIÇOS.....	15
3 COMANDOS BÁSICO DO EDITOR VIM.....	15
4 CONFIGURANDO DHCP.....	15
5 INICIANDO SERVIÇO NAMED.....	16
6 CONFIGURANDO SQUID.....	16
7 CRIANDO SCRIPT FW.SH.....	18
8 CONFIGURANDO RELATÓRIO COM SARG.....	20
9 SINCRONIZAÇÃO AUTOMÁTICA DO RELÓGIO.....	24
10 ALTERAR PORTA PADRÃO DO SSH.....	24
11 ADICIONANDO BLOQUEIOS DE SITES E DOWNLOADS.....	24

MANUAL DE INSTALAÇÃO E CONFIGURAÇÃO DE FIREWALL – CENTOS

1 INSTALANDO CENTOS

Toda instalação será feita utilizando a distribuição CentOS 5.7 em modo texto, também pode ser instalado na versão gráfica (normalmente não utilizada), é necessário que o firewall tenha duas placas de redes, uma irá receber o ip da operadora ou prestadora de serviço e a outras placa será utilizada para comunicação na rede local e acesso dos clientes em direção a internet.

Abaixo segue os passos para instalação do CentOS 5.7.



Welcome to CentOS



<Tab>/<Alt-Tab> between elements ; <Space> selects ; <F12> next screen

Welcome to CentOS

Language Selection

What language would you like to use during the installation process?

- Polish
- Portuguese
- Portuguese(Brazilian)**
- Punjabi
- Russian
- Serbian
- Serbian(Latin)
- Sinhala

OK **Back**

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Bem-vindo ao CentOS

Seleção de Teclado

Qual tipo de teclado está conectado a este computador?

- ar-digits
- ar-qwerty
- ar-qwerty-digits
- be-latin1
- ben
- ben-probhat
- bg
- br-abnt2**

OK **Voltar**

<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar

Bem-vindo ao CentOS

Aviso

Nao foi possível ler a tabela de partições do dispositivo sda (ATA UBOX HARDDISK 8189 MB). Para criar novas partições o mesmo precisa ser inicializado, causando a perda de TODOS OS DADOS nele contidos.

Esta operação anula quaisquer escolhas de instalação prévias referentes a quais dispositivos devem ser ignorados.

Você deseja inicializar este disco, apagando TODO OS DADOS?

Sim

Nao

<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar
Bem-vindo ao CentOS

Tipo de Particionamento

A instalação requer o particionamento do seu disco rígido. Por padrão, um layout de particionamento é escolhido, o qual atende a maioria dos usuários. Você pode escolher usar este ou criar o seu próprio.

Apagar todas partições nos discos selecionados e criar layout padrão.
Remover partições Linux nos discos selecionados e criar layout padrão.
Usar espaço livre nos discos selecionados e criar layout padrão.
Criar layout personalizado.

Que disco(s) você deseja utilizar para esta instalação?

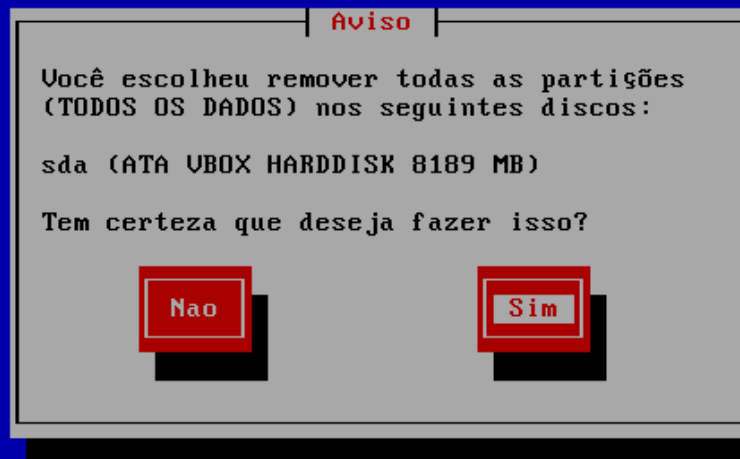
[*] sda 8189 MB (ATA UBOX HARDDISK)

OK

Voltar

<Espaço>,<+>,<-> seleção | <F2> Adicionar drive | <F12> continuar

Bem-vindo ao CentOS



<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar
Bem-vindo ao CentOS



<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar

Bem-vindo ao CentOS

Configuração de rede para eth0

Intel Corporation 82540EM Gigabit Ethernet Controller
08:00:27:E5:7A:C6

- Ativar na Inicialização
- Habilitar suporte para IPv4
- Habilitar suporte para IPv6

<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar
Bem-vindo ao CentOS

Configuração de IPv4 para eth0

Intel Corporation 82540EM Gigabit Ethernet Controller
08:00:27:E5:7A:C6

- Configuração de IP dinâmico (DHCP)
- Configuração de endereço manual

Endereço IP / Prefixo (Máscara de Rede)
----- / -----

<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar

Bem-vindo ao CentOS

Configuração de IPv4 para eth1

Intel Corporation 82540EM Gigabit Ethernet Controller
08:00:27:0C:BD:45

() Configuração de IP dinâmico (DHCP)
(*) Configuração de endereço manual

Endereço IP	Prefixo (Máscara de Rede)
192.168.0.1	255.255.255.0

OK **Voltar**

<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar
Bem-vindo ao CentOS

Configuração de Rede

A configuração atual para cada interface está listada próxima ao nome do dispositivo. Interfaces desconfiguradas são exibidas como DESCONFIGURADAS. Para configurar uma interface, realce-a e escolha Editar. Quando terminar, pressione OK para continuar.

eth0: Ativado na Inicialização , DHCP
eth1: Ativado na Inicialização , 192.168.0.1
⋮

Editar **OK** **Voltar**

<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar

Bem-vindo ao CentOS

Configuração do nome de host

Se o seu sistema faz parte de uma rede grande na qual os nomes das máquinas são atribuídos pelo DHCP, selecione 'automaticamente via DHCP'. Caso contrário, selecione 'manualmente' e indique o nome de host para seu sistema. Se você não o fizer, seu sistema será conhecido como 'localhost'.

automaticamente via DHCP
 manualmente

<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar

Bem-vindo ao CentOS

Seleção de Fuso Horário

Em que fuso horário você está localizado?

O relógio do sistema utiliza o UTC

- America/Santa_Isabel
- America/Santarem
- América/Santiago
- América/Santo Domingo
- América/Sao Paulo

<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar

Bem-vindo ao CentOS

Senha do Root (Administrador)

Escolha uma senha para o root. Você deverá digitá-la duas vezes para garantir que não há erros. Lembre-se que a senha do root, por ser a senha do administrador, é uma parte crítica da segurança do seu sistema!

Senha: *****
Senha (confirmar): *****

<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar
Bem-vindo ao CentOS

Seleção de pacotes

A instalação padrão do CentOS inclui um conjunto de programas aplicáveis para uso geral na Internet. Quais tarefas adicionais você gostaria que seu sistema suportasse?

- Desktop - Gnome
- Desktop - KDE
- Server
- Server - GUI

Personalizar seleção de programas

<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar

Bem-vindo ao CentOS

Instalação prestes a começar

Um relatório completo da sua instalação estará em /root/install.log após reinicializar seu computador. Talvez você queira guardar este arquivo para futura referência.

OK **Voltar**

<Tab>/<Alt-Tab> alterna seleção | <Espaço> seleciona | <F12> continuar
Bem-vindo ao CentOS

Concluído

Parabéns, sua instalação do CentOS está completa.

Remova qualquer mídia utilizada no processo de instalação e pressione <Enter> para reinicializar seu sistema.

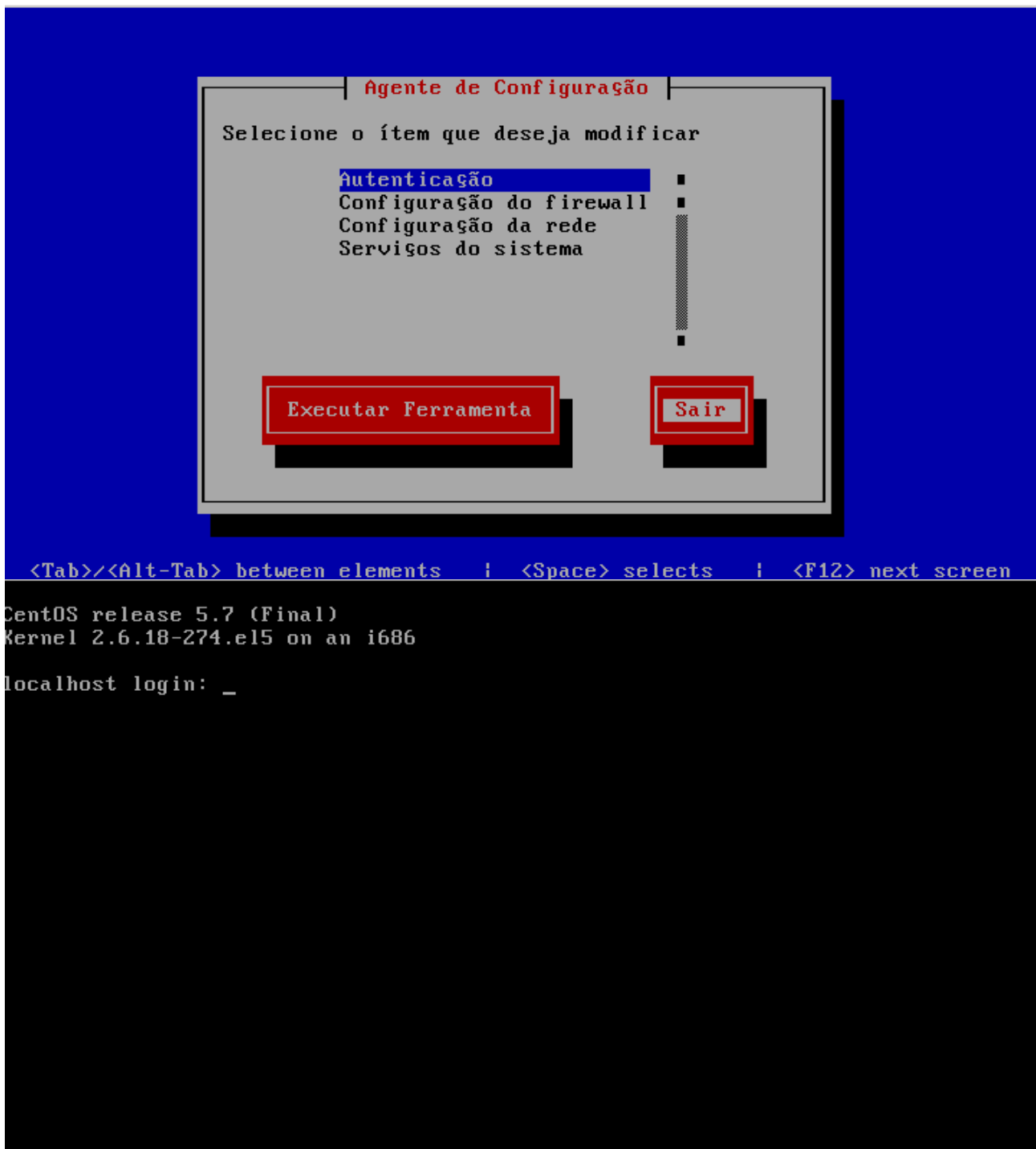
Reinicializar

4206 (ms)

ation:

<Enter> para reinicializar

Se todos os passos ocorrerem de maneira satisfatória será apresentada a tela para reinicializar o sistema, após o reinício do sistema será necessário a instalação e configuração dos serviços, que são necessário para o funcionamento do firewall.



Tela de Login do CentOS.

Usuário: root

Senha: [senha_definida_na_instalação]

Verifique o ip das interfaces com o comando **ifconfig**.

```

eth0      Link encap:Ethernet  Endereço de HW 08:00:27:E5:7A:C6
          inet end.: 10.0.20.157  Bcast:10.0.20.255  Masc:255.255.255.0
          UP BROADCASTRUNNING MULTICAST  MTU:1500  Métrica:1
          RX packets:3874 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:331623 (323.8 KiB)  TX bytes:3313 (3.2 KiB)

eth1      Link encap:Ethernet  Endereço de HW 08:00:27:0C:BD:45
          inet end.: 192.168.0.1  Bcast:192.168.0.255  Masc:255.255.255.0
          UP BROADCASTRUNNING MULTICAST  MTU:1500  Métrica:1
          RX packets:3725 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:321743 (314.2 KiB)  TX bytes:2525 (2.4 KiB)

lo        Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          UP LOOPBACKRUNNING  MTU:16436  Métrica:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:0
          RX bytes:560 (560.0 b)  TX bytes:560 (560.0 b)

[root@localhost ~]#

```

Nesse caso a interface ETH0 recebeu um ip automático de um modem adsl e a interface ETH1 está com o ip que será usado para rede local.

Deve-se adaptar o endereço da interface do firewall de acordo com a faixa de rede utilizada na rede interna, caso a rede já venha sendo utilizada.

Teste a conectividade do firewall com a internet com o comando `ping -c 3 www.google.com.br`

Caso a resposta seja positiva seu firewall está comunicando com a internet e poderá ser instado os serviços necessários para conclusão da instalação do firewall, conforme a imagem abaixo.

```

[root@localhost ~]# ping -c 3 www.google.com.br
PING www.l.google.com (74.125.234.81) 56(84) bytes of data:
64 bytes from gru03s07-in-f17.1e100.net (74.125.234.81): icmp_seq=1 ttl=54 time=
30.5 ms
64 bytes from gru03s07-in-f17.1e100.net (74.125.234.81): icmp_seq=2 ttl=54 time=
32.8 ms
64 bytes from gru03s07-in-f17.1e100.net (74.125.234.81): icmp_seq=3 ttl=54 time=
30.8 ms

--- www.l.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2081ms
rtt min/avg/max/mdev = 30.578/31.436/32.899/1.049 ms
[root@localhost ~]#

```

2 INSTALANDO SERVIÇOS

Para instalação dos serviços necessários do firewall, iremos usar o comando **yum install** conforme abaixo. Também é necessário que o firewall tenha conectividade com a internet para poder prosseguir com a instalação dos serviços.

Os comandos no linux são case-sensitive, ou seja, eles diferenciam letras maiúsculas e minúsculas.

```
[root@localhost ~]# yum install httpd squid ntp dhcp bind bind-chroot caching-nameserver gcc gcc-c++ -y
```

Após a instalação é necessário ativar os serviços para que sejam inicializados automaticamente no carregamento do sistema.

```
[root@localhost ~]# chkconfig httpd on
[root@localhost ~]# chkconfig squid on
[root@localhost ~]# chkconfig dhcpd on
[root@localhost ~]# chkconfig named on
```

3 COMANDOS BÁSICO DO EDITOR VIM

Para configurar os arquivos é necessário saber alguns comandos básico do editor VIM.

Abrir um arquivo com o editor vim

```
[root@localhost ~]# vim /caminho/arquivo.conf
```

Iniciar inserção de texto

[TECLA INSERT]

Retornar ao modo de comandos

[TECLA ESC]

Movimentação dentro do arquivo

[SETA PARA CIMA]

[SETA PARA BAIXO]

[SETA PARA DIREITA]

[SETA PARA ESQUERDA]

Para salvar o arquivo

[TECLA SHIFT] :w

Para salvar o arquivo e sair do editor

[TECLA SHIFT] :wq

4 CONFIGURANDO DHCP

Para que os computadores na rede utilizem um endereço ip automaticamente, é necessário

configurar o serviço de dhcp no firewall.

Cópia de segurança do arquivo dhcpd.conf

```
[root@localhost ~]# cp /etc/dhcpd.conf /etc/dhcpd.conf.original
```

Configuração do arquivo dhcpd.conf

```
[root@localhost ~]# vim /etc/dhcpd.conf
```

Adicione as seguintes linhas

```
ddns-update-style interim;
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.0.255;
option routers 192.168.0.1;
option domain-name-servers 192.168.0.1, 8.8.8.8, 8.8.4.4;

subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.1 192.168.0.254;
}
```

Com a arquivo configurado inicie o serviço com o comando abaixo.

```
[root@localhost ~]# service dhcpd start
```

```
[root@localhost ~]# service dhcpd start
Iniciando dhcpd: [ OK ]
[root@localhost ~]# _
```

5 INICIANDO SERVIÇO NAMED

Para iniciar a resolução de nomes DNS na rede interna para internet, ative o serviço com o comando abaixo.

```
[root@localhost ~]# service named start
```

```
[root@localhost ~]# service named start
Iniciando named: [ OK ]
[root@localhost ~]# _
```

6 CONFIGURANDO SQUID

Agora configurando o arquivo padrão utilizado pelo squid, ele funcionará com a porta 3128 no modo de escuta.

Cópia de segurança.

```
[root@localhost ~]# cp /etc/squid/squid.conf /etc/squid/squid.conf.original
```


Criação do arquivo squid.conf

```
[root@localhost ~]# vim /etc/squid/squid.conf
```

O uso da # faz com que a linha fique comentada sendo ignorada suas configurações e também é utilizada para colocar comentários como este.

```
http_port 3128 transparent
```

```
visible_hostname Firewall
```

```
# Proxy transparent com autenticação não funciona
```

```
error_directory /usr/share/squid/errors/Portuguese/
```

```
cache_mem 64 MB
```

```
maximum_object_size_in_memory 64 KB
```

```
maximum_object_size 512 MB
```

```
minimum_object_size 0 KB
```

```
cache_swap_low 50
```

```
cache_swap_high 70
```

```
cache_dir ufs /var/spool/squid 4096 16 256
```

```
cache_access_log /var/log/squid/access.log
```

```
#cache_store_log /var/log/squid/store.log
```

```
#cache_swap_log /var/log/squid/cache_swap.log
```

```
refresh_pattern ^ftp: 15 20% 2280
```

```
refresh_pattern ^gopher: 15 0% 2280
```

```
refresh_pattern . 15 20% 2280
```

```
acl all src 0.0.0.0/0.0.0.0
```

```
acl manager proto cache_object
```

```
acl localhost src 127.0.0.1/255.255.255.255
```

```
acl SSL_ports port 22 995 993 465
```

```
acl Safe_ports port 21 80 138 139 443 563 70 210 280 488 59 777 901 1025-65535
```

```
acl purge method PURGE
```

```
acl CONNECT method CONNECT
```

```
http_access allow manager localhost
```

```
http_access deny manager
```

```
http_access allow purge localhost
```

```
http_access deny purge
```

```
http_access deny !Safe_ports
```

```
http_access deny CONNECT !SSL_ports
```

```
# Validação da rede local
```

```
acl redelocal src 192.168.0.0/24
```

```
# Bloqueio de sites por dominio
```

```
#acl sites url_regex -i "/etc/squid/bloqueados/sites"
```

```
#http_access deny sites
```

```
#acl porno url_regex -i "/etc/squid/bloqueados/porno"
```

```
#http_access deny porno
```

```
# Bloqueio de arquivos por extensão
```

```
#acl extensao urlpath_regex -i "/etc/squid/bloqueados/extensao"
```

```
#http_access deny extensao
```

```

# Controle de banda de acesso a internet
# 15728640 = 15Mb de banda total contratada junto a operadora = 1,5MB/s
# 1048576 = 1Mb de banda controlada = 128Kb/s de velocidade máxima de download por
usuário
# 2097152 = 2mb de banda controlada = 256Kb/s de velocidade máxima de donwload por
usuário
#delay_pools 1
#delay_class 1 2
#delay_parameters 1 15728640/15728640 1048576/1048576
#delay_parameters 1 -1/-1 15728640/15728640 1048576/1048576 # 0 -1/-1 é ilimitado o
uso da banda
#delay_parameters 1 32000/32000 1048576/1048576
#delay_access 1 allow redelocal

http_access allow localhost
http_access allow redelocal
http_access deny all

```

Com o arquivo padrão configurado, inicie o serviço para testar se tudo está configurado de maneira correta com o comando abaixo.

```
[root@localhost ~]# service squid start
```

```

[root@localhost ~]# vim /etc/squid/squid.conf
[root@localhost ~]# service squid start
init_cache_dir /var/spool/squid... Iniciando squid: ..      [ OK ]
[root@localhost ~]# _

```

Verifique se o squid está funcionando com o comando abaixo.

```
[root@localhost ~]# netstat -antp | grep squid
```

```

[root@localhost ~]# netstat -antp | grep squid
tcp        0      0 0.0.0.0:3128          0.0.0.0:*           LISTEN      2891/(squid)
[root@localhost ~]# _

```

Caso exiba uma mensagem de erro tente o comando abaixo e verifique o arquivos de configuração do squid.

```
[root@localhost ~]# service squid restart
```

7 CRIANDO SCRIPT FW.SH

Agora precisamos configurar o arquivo de script para inicializar as regras do firewall.

```
[root@localhost ~]# vim /etc/squid/fw.sh
```

Adicione as linhas a seguir

```

#!/bin/bash
    echo Inicializando regras do firewall
    sleep 0

IF_WAN=eth0 # INTERFACE DE SAIDA PARA INTERNET
LAN=192.168.0.0/24 # ENDEREÇO PARA REDE LOCAL LAN

# LIMPA REGRAS DO FIREWALL
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -F
iptables -t nat -F

# SERVIDORES DNS LOCAL E EXTERNO
echo "nameserver 127.0.0.1" > /etc/resolv.conf
echo "nameserver 8.8.8.8" >> /etc/resolv.conf
echo "nameserver 8.8.4.4" >> /etc/resolv.conf

# ATIVA O SISTEMA DE ROTEAMENTO DE PACOTES
echo 1 > /proc/sys/net/ipv4/ip_forward

# ATIVA O MODO DE MASQUERADE
iptables -t nat -A POSTROUTING -o $IF_WAN -j MASQUERADE # Mascaramento
de rede

# FORÇA A NAVEGACAO PELA PORTA 3128
# A LINHA A SEGUIR SÃO NECESSÁRIAS PARA NAVEGAÇÃO NA INTERNET
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 80 -s $LAN -j REDIRECT --to
3128 # Forca navegacao na 3128

# BLOQUEIO DA PORTA 1863 - MSN
iptables -t nat -A PREROUTING -p tcp -s $LAN --dport 1863 -j DROP

# BLOQUEANDO SITE COM HTTPS
#cat /etc/squid/bloqueados/bloq_https | while read SITES;
# do
#   iptables -A FORWARD -p tcp -d $SITES -j ACCEPT
# done

```

Caso todos os passos acima tenham sido realizados com sucesso, conecte o um computador na interface que irá atender a rede local e verifique se conseguirá acessar a internet. Caso tenha sucesso, todos os computadores que estiverem conectados após a implantação, conseguirão navegar na internet sem nenhuma restrição de acesso.

Se por algum motivo retornar alguma mensagem de erro ou não for possível a navegação na internet, é necessário revisar todos os pontos deste documento.

Agora deverá ser adiciona o script do firewall para inicializar com o sistema.

Abra o arquivos rc.local.

[root@localhost ~]# vim /etc/rc.local

Adicione a linhas abaixo.

```
sh /etc/squid/fw.sh
```

Reinicie o Linux com o comando **reboot** e verifique se conseguirá navegar na internet.

8 CONFIGURANDO RELATÓRIO COM SARG

Após o firewall estar instalado e configurado corretamente é interessante que o administrador utilize alguma ferramenta para verificar os endereços e sites que os usuários estão acessando para adicionar na lista de sites que serão bloqueados posteriormente.

Faça o download do sarg no endereço abaixo:

```
[root@localhost ~]# wget http://sourceforge.net/projects/sarg/files/sarg/sarg-2.3.1/sarg-2.3.1.tar.gz
```

Descompacte o arquivo com o comando.

```
[root@localhost ~]# tar xvf sarg-2.3.1.tar.gz
```

Entre no diretório do sarg

```
[root@localhost ~]# cd sarg-2.3.1
```

Faça a compilação do programa

```
[root@localhost ~]# ./configure
```

```
[root@localhost ~]# make
```

```
[root@localhost ~]# make install
```

```
[root@localhost ~]# sarg
```

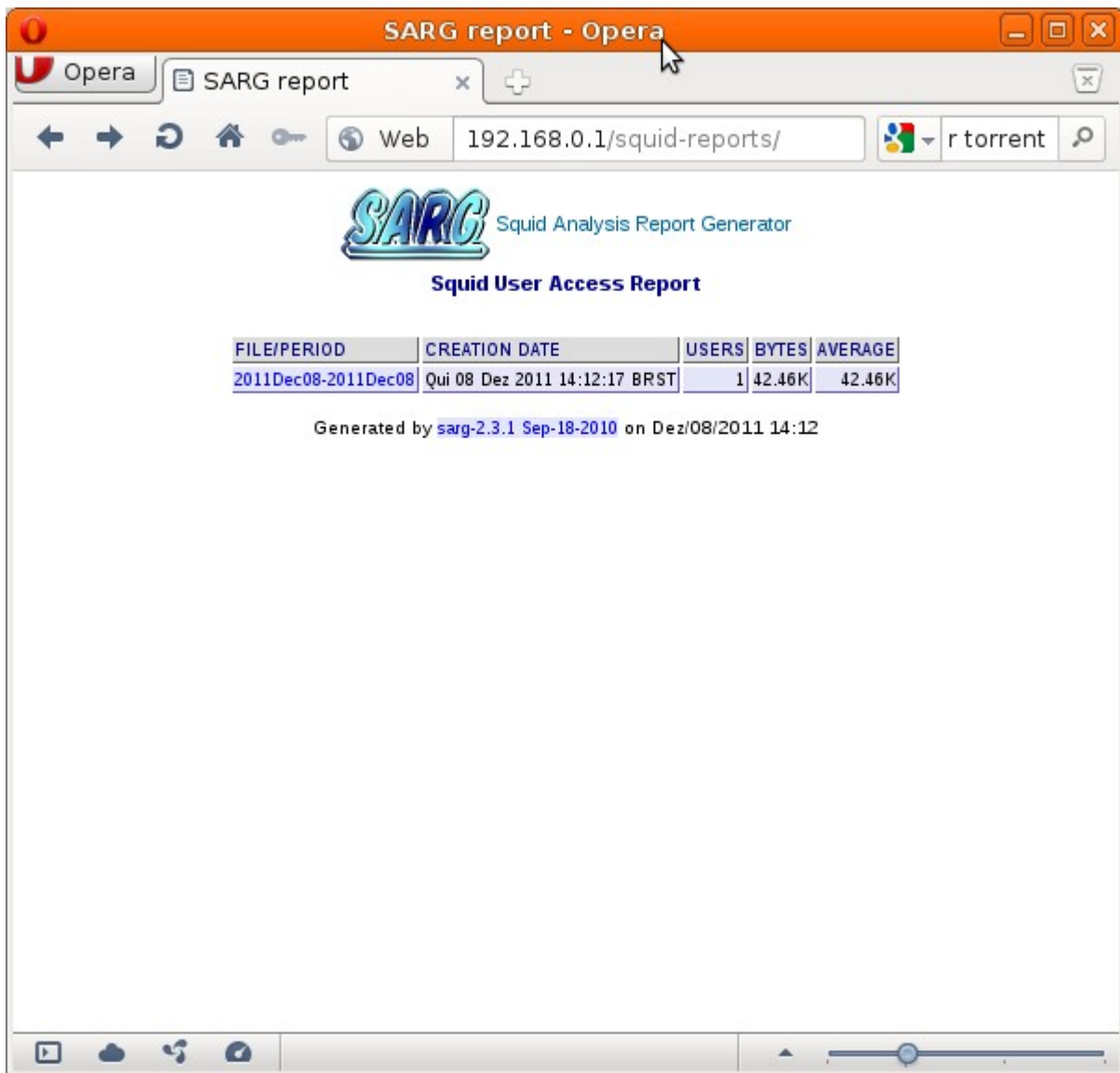
Caso queira gerar os relatórios manualmente antes do horário definido para execução automática, digite **sarg** na linha de comando do Linux.

Após estes procedimentos a compilação e instalação terá terminada, caso tenha retornado alguma mensagem de erro, é necessário verificar se os comandos foram digitados de maneira correta.

Para verificar se tudo está funcionando de maneira correta, com um computador conectado na placa de rede, que será usada para rede local, abra o navegador e coloque o endereço ip configurado para rede interna, nesse caso foi usado 192.168.0.1 adicionando a pasta de relatórios do squid.

```
http://192.168.0.1/squid-reports
```

O resultado será semelhante a imagem abaixo



Por padrão o sarg não possui senha de acesso, que no quesito segurança isso não é aconselhável, pois qualquer computador poderia acessar os relatórios.

Por medidas de segurança será colocado senha de acesso aos relatórios do sarg.

Vamos editar o arquivo de configuração do http.

```
[root@localhost ~]# vim /etc/httpd/conf/httpd.conf
```

Devemos alterar a linha abaixo

```
Listen 80
```

Para

```
Listen 8082
```

Adicione as linhas abaixo no final do arquivo de configuração.

```
<Directory "/var/www/html/squid-reports/">  
Options Indexes MultiViews
```

```
AllowOverride None
Order allow,deny
Allow from all
AuthType Basic
AuthName "Acesso Restrito"
AuthUserFile "/etc/squid/.sargpasswd"
Require valid-user
</Directory>
```

Salve as configurações, feche o arquivo e reinicie o serviço httpd com o comando abaixo.

```
[root@localhost ~]# service httpd restart
```

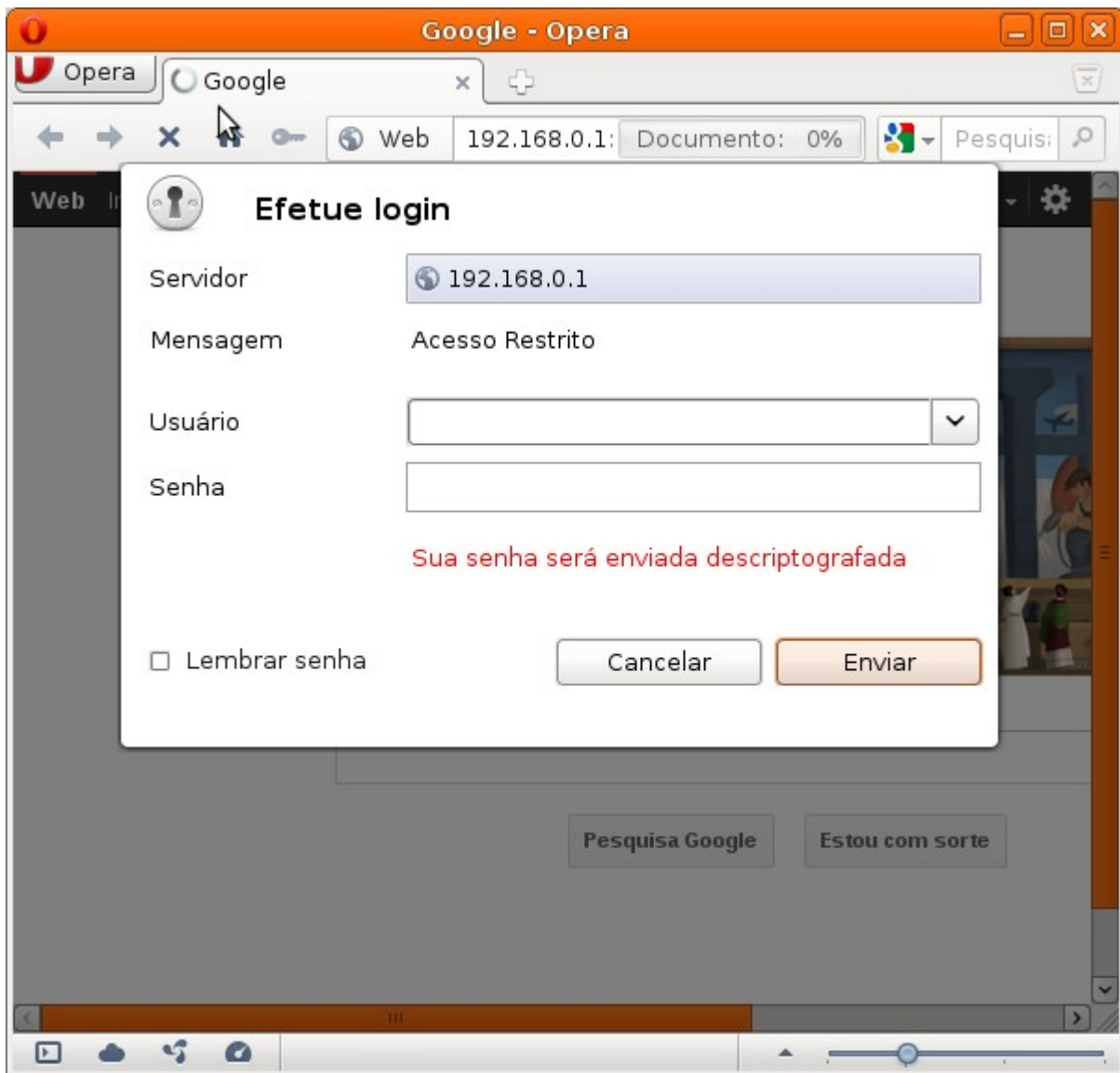
Com isso já temos um sistema de autenticação para os relatórios, porém é preciso criar um usuário para acessá-lo e será feitos com os comandos abaixo.

```
[root@localhost ~]# htpasswd -c /etc/squid/.sargpasswd root
```

```
[root@localhost etc]# htpasswd -c /etc/squid/.sargpasswd root
New password:
Re-type new password:
Adding password for user root
[root@localhost etc]# _
```

Digite a senha para acesso, poderá ser a mesma senha do administrador root.

Abra novamente o navegador e adicione digite o endereço <http://192.168.0.1:8082/squid-reports/>



Deverá ser mostrado um tela de login para digitação do usuário e senha, caso tenha ocorrido tudo normalmente, o sistema de relatórios do squid está configurado bastando apenas adicionar o squid para emissão dos relatórios diários.

Para adicionar o script para gerar relatórios diários siga os passos abaixo.

```
[root@localhost ~]# vim /etc/squid/relatorio.sh
```

Adicione as linhas abaixo

```
clear  
DATA=`date +%d/%m/%Y`  
sarg -g e -d $DATA'-$DATA
```

Salve e feche o arquivo de relatório.

Adicione o script para execução todos os dias em um determinado horário, nesse caso será colocado todos os dias as 23:00 Hrs.

Execute o comando abaixo.

```
[root@localhost ~]# crontab -e
```

Adicione a linha abaixo.

```
00 23 * * * * /etc/squid/relatorio.sh
```

A partir desse momento serão gerados relatórios todos os dias as 23:00 Hrs.

9 SINCRONIZAÇÃO AUTOMÁTICA DO RELÓGIO

Para atualizar automaticamente o relógio do firewall, crie um arquivo com nome clock.sh na pasta /etc/squid/

```
[root@localhost ~]# vim /etc/squid/clock.sh
```

Adicione a linha abaixo

```
ntpdate -u pool.ntp.org
```

Adicione a sincronização todos os dias as 23:00

```
[root@localhost ~]# crontab -e
```

Adicione a linha abaixo.

```
00 00 * * * * /etc/squid/clock.sh
```

10 ALTERAR PORTA PADRÃO DO SSH

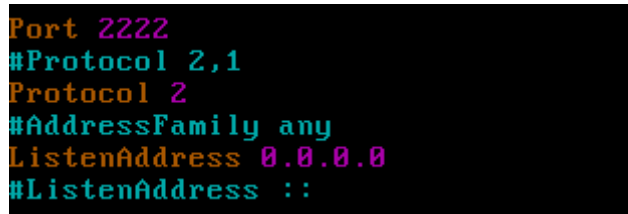
Por padrão o acesso remoto ssh está confirado na porta 22 e devemos mudá-la, não é necessário mas é interessante pois aumentará mais a segurança.

Para isso vamos editar o arquivo padrão do ssh.

```
[root@localhost ~]# vim /etc/ssh/sshd_config
```

Descomente a linha abaixo e mude-a para 2222

Descomente a linha ListenAddress 0.0.0.0



```
Port 2222
#Protocol 2,1
Protocol 2
#AddressFamily any
ListenAddress 0.0.0.0
#ListenAddress ::
```

11 ADICIONANDO BLOQUEIOS DE SITES E DOWNLOADS

Como a proposta de um firewall é ter controle de acessos a determinados sites, de nada adiantaria ter configurado e não adicionar a lista dos sites que serão bloqueados os acessos. Devemos criar uma lista de sites e adicionar nos arquivos de listagem que serão criados a partir

desse ponto.

Devemos criar alguns arquivos, e acioná-los no arquivo de configuração do squid.
Para criar os arquivos execute os comandos abaixo.

```
[root@localhost ~]# mkdir /etc/squid/bloqueados
[root@localhost ~]# touch /etc/squid/bloqueados/porno
[root@localhost ~]# touch /etc/squid/bloqueados/chat
[root@localhost ~]# touch /etc/squid/bloqueados/sites
[root@localhost ~]# touch /etc/squid/bloqueados/extensao
```

Poderá ser criados diversos outros tipo de arquivos, grupos, pastas separadas, fica de acordo com que for mais fácil de trabalhar.

Após criar os arquivos devemos adicionar os sites nos arquivos **porno**, **chat**, **sites** e as extensões que serão bloqueadas para download no arquivos **externsão**.

Adicione os site que serão bloqueados.

```
[root@localhost ~]# vim /etc/squid/bloqueados/porno
```

Salve o arquivo e saia.

Repita o processo nos outros arquivos.

```
[root@localhost ~]# vim /etc/squid/bloqueados/chat
```

Salve o arquivo e saia.

Repita o processo nos outros arquivos.

```
[root@localhost ~]# vim /etc/squid/bloqueados/sites
```

Salve o arquivo e saia.

Adicione as extensões de arquivos que serão bloqueados..

```
[root@localhost ~]# vim /etc/squid/bloqueados/extensao
```

Salve o arquivo e saia.

Após criado a lista do que será bloqueado pelo firewall, devemos habilitar as linha dentro do arquivos do squid.

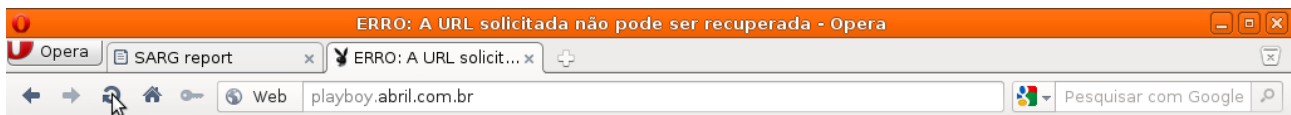
```
[root@localhost ~]# vim /etc/squid/squid.conf
```

```
# Bloqueio de sites por dominio
acl porno url_regex -i "/etc/squid/bloqueados/porno"
http_access deny porno

# Bloqueio de arquivos por extensão
acl extensao urlpath_regex -i "/etc/squid/bloqueados/extensao"
http_access deny extensao
```

Reinicie o serviço do squid e teste no navegador se os sites da lista estão sendo bloqueados.

Se as configurações estiverem corretas será mostrado a imagem abaixo caso alguns usuário tente acessar algum dos sites que estiverem na lista dos bloqueados.



ERRO

A URL solicitada não pode ser recuperada

Na tentativa de recuperar a URL: <http://playboy.abril.com.br/>

O seguinte erro foi encontrado:

- **Proibido o Acesso.**

O controle de acessos impediu sua requisição. Caso você não concorde com isso, por favor, contate seu provedor de serviços, ou o administrador de sistemas.

Generated Thu, 08 Dec 2011 17:53:39 GMT by Firewall_Delta (squid/2.6.STABLE21)



Esta página de ACCESS DENIED poderá ser personalizada, basta editar o arquivo ERR_ACCESS_DENIED dentro da pasta /etc/share/squid/errors/Potuguese/ caso altere a linha no arquivo squid.conf para outro idioma deverá entrar na pasta equivalente ao idioma configurado no squid.conf